THE FUTURE OF POSSIBLE

A DJI Technology Whitepaper

# "What's In a Name?"

## A Call for a Balanced Remote Identification Approach

March 22, 2017

* * *

## The Utility of Remote Identification Technologies

Section 2202 of the 2016 FAA Extension Act contemplates the development of remote identification technologies for unmanned aircraft systems (UAS). Regulatory proposals in Europe, including from the European Aviation Safety Agency (EASA), and in European Union member states such as France and Germany, have also called for remote identification technology. Indeed, Italy and Denmark apparently already mandate these technologies, in regulations that seem not to be enforced because the means of compliance do not yet exist. Remote identification is potentially a problem-solving approach to addressing policy concerns including security and accountability.

DJI believes that laws of general applicability should apply to drones, just as they do to other technologies. For example, a law that makes unlawful surveillance illegal should apply to misconduct using drones as it would apply to misconduct using other types of cameras. These laws of general applicability have been created by lawmakers over decades and balance competing interests including privacy interests, community values, national legal traditions, cultural norms, the First Amendment (and similar doctrines outside the United States), and journalism interests, among others. The balance reached after decades of legislation and jurisprudence should not be disrupted each time a new technology comes along. Operational rules relating to UAS obviously apply as well.

In our many discussions with policymakers and community members around the world, a theme has emerged about one way in which drones are different from many other technologies: the remoteness of the operator. Unlike manned aircraft, automobiles, mobile telephones with cameras, and other imaging devices, drones are remotely operated. In many cases, particularly in jurisdictions limiting operations to visual line of sight, the operator is near the unmanned aircraft while in flight and it is not difficult to locate her. In some instances, she is not. In those

instances, if the operator is actually doing something that everyone would readily agree is unlawful, there is an accountability challenge. Remote identification, properly and reasonably deployed, could significantly help to address that challenge. It might also provide a measure of social comfort to those who are unfamiliar with the technology and have anxieties about its use, founded or unfounded. For security agencies protecting sensitive locations, being able to identify UAS that are cooperating with an identification regime can suggest a tactical response to approaching UAS that are not cooperating. For these reasons, DJI supports the concept of remote identification. However, we urge that the development and implementation of such a mechanism be thoughtful, tailored to address and solve the actual challenge, and take into consideration other important interests.

**The Privacy Interests of the Operator**

We have observed that the privacy interests of the drone operator are often not considered, or even raised, in policy discussions about remote identification. These interests are significant and must be taken into account. Across our hundreds of thousands of customers, we have heard from companies and individuals who have serious and legitimate concerns about the confidentiality of their drone operations. By way of example, here are a few types of operations that raise competitive business or other operator privacy concerns:

- An alternative energy company scouting out a prospective new wind farm location
- A seed company flying regular missions to measure the performance of its newest type of seed crop
- A teenager in her backyard operating a drone for a school science project
- A technology firm surveying and mapping land for its new corporate campus
- A drone company developing and testing the latest forthcoming product
- An insurance adjuster inspecting a storm-damaged property to guard against fraudulent claims
- A journalist engaged in investigative journalism
- A drone service company that closely guards information on how many operations it conducts each week relative to its competitors

These are all examples of companies and individuals who have a legitimate reason not to have their operations of UAS tracked and recorded, or otherwise made available to far-away observers who may include competitors. These concerns are analogous to ones in other domains. We do not constantly track and record the location of motor vehicles, even though doing so would lead to near-perfect enforcement of motor vehicle laws (the violation of which costs lives each day). Manned aircraft are not subject to constant surveillance and tracking. In Class G airspace, which is much of the country, no flight plan is required, and radar may not be active to event detect the presence of the aircraft. In vast areas of the country, it is possible for a pilot to fly from one farm's grass strip to another, and back again, without anyone else having access to that flight information including the identity of the pilot. Even when manned aircraft are close enough to be visually identified by their marked N number, the economics of aircraft ownership compel limited liability corporations (LLCs) to protect the identity of the owner. And even with the

aircraft owner's name in hand, it is not possible to learn who was flying the aircraft or why they were operating without making an inquiry with the owner.

A significant effort to protect against public dissemination of flight tracking data resulted in the Block Aircraft Registration Request (BARR) program enabled by Congress in the April 2000 Wendell H. Ford Aviation Investment and Reform Act for the 21st Century, Pub. Law 106-181, Section 729.

In 2011, changes to the BARR program were considered in an FAA Notice of Proposed Modification to the June 1, 2006 MOA FAA/Subscriber Memorandum of Agreement for ASDI/NASSI Industry Access and Request for Comments, FAA docket number FAA-2011-0183. FAA received approximately 630 written comments.

In these comments, organizations such as NBAA and AOPA noted that making an aircraft's use public compromises its value as a business tool and exposes competitively sensitive information. A selection of these comments are provided in Appendix B. Final guidance on this topic was published by the FAA in 2013.

Operators of unmanned aircraft have many of the same interest in privacy, and are poised to make even greater use of them as a business tool than manned aircraft which they now outnumber. Although UAS do not carry people, and so do not implicate free movement of people, identification information does indicate the location of the person operating the UAS, thus revealing the activities of persons and businesses.

The interest in privacy is, unfortunately, arguably heightened compared to manned aircraft considering the occasional violent confrontations that UAS operators have faced over the last few years, including physical assault and gunfire. A system that enables belligerent individuals to look up the name and address of, and then knock on the door of, a local UAS operator, is not acceptable and will detrimentally impact UAS operators who are operating safely and doing nothing wrong. The personal information of the owner (or operator) should be accessible to law enforcement only, who can investigate complaints of unlawful or dangerous conduct. Privacy and personal safety interests compel an identification system that protects operator business interests and discloses personally identifiable information only to law enforcement agencies.

**The Balanced Approach: Non-Networked, Localized ID**

The balanced approach that we propose to solving safety, security, and accountability concerns while taking into account operator privacy and safety, is to create an identification mechanism that provides localized identification without permanent recording or logging. Remote UAS identification then becomes analogous to an enhanced version of a car license plate. An identifier, such as a registration number, together with position information about the drone, and perhaps some voluntary information if the operator wishes, is transmitted from the drone, and is available to all receivers that are within range. Authorized receivers of the transmission who believe the drone's operator is violating a regulation or engaged in unlawful acts can record and investigate, similar to how a license plate might be recorded by someone who is cut off on a

road. Radio-based identification is actually better than license plates; it will work through walls, at greater distances of likely more than a mile given current technologies. In contrast, a license plate is readable from only a few dozen feet away.

This localized approach is preferred to networked solutions, which raise a number of concerns. A networked solution requires network connectivity, most typically via mobile phone. There are various locations that lack reliable data signals, which would thwart the ID system, as well as provide an excuse to a non-compliant operator. A networked solution also inherently raises the possibility that all UAS operations will be tracked and recorded for future unknown exploitation, including enforcement quotas or business espionage. A networked system is also susceptible to system-wide hacking, or the creation by detractors of false entries of drone operations that do not exist.

No other technology is subject to mandatory industry-wide tracking and recording of its use, and we strongly urge against making UAS the first such technology. The case for such an Orwellian model has not been made. Certainly, we have yet to hear why anyone in Detroit would need to know who is operating a drone in Denver, or why. A networked system provides more information than needed, to people who don't require it, and exposes confidential business information in the process.

A non-networked primary solution is also easier to implement because it can be done by a single industry constituent who are well positioned to implement it: the manufacturers. Networked solutions require the manufacturers, data providers, a server resource, the operator, and the designated receiver of the ID information to *all* create something that works together, and to maintain and pay for the upkeep of all the parts (or impose this cost on the operators). Even if that system could be devised, it will take longer to implement. The best solution is usually the simplest. The focus of the primary method for remote identification should be on a way for anyone concerned about a drone flight in close proximity to report an identifier number to the authorities, who would then have the tools to investigate the complaint without infringing on operator privacy.

**Available Technologies Already Exist**

The key to deploying a viable identification system is to leverage and primarily focus on technology that already exists as the primary method. UAS in widespread use today already transmit data at significant range, using their command and control and video transmission links. We propose use of protocols within the existing C2 or video link to transmit identification information to ground receivers. These control and video links most often make use of the 2.4 GHz and 5.8 GHz bands. To facilitate widespread adoption of this approach, DJI proposes creating at least one open identification protocol for UAS that use wifi control links, in addition to protocols that might be developed for other UAS using other control links. Given the life cycle of this technology, in which we estimate that the typical drone operator purchases a new model within approximately one year, it ought not be difficult for manufacturers to modify existing radio transmission protocols to broadcast identification information, and for the majority of the users to be using the technology within a matter of months from the initial rollout.

For UAS operators who choose to build their own UAS, add-on RF modules may be made available including those that leverage other existing protocols such as Bluetooth; however we find that add-on modules are disfavored for ready-to-fly products because of potentially undesired performance impact on the operation of the UAS (such as radio interference, balance and aerodynamic impacts) for which a manufacturer should not be held responsible. Additionally, for those less concerned about tracking and privacy, or who do not wish to use radio identification technologies or add-on modules, a networked alternative system could be made available, but it should be secondary and optional.

Thus, we propose in concept the following remote identification solutions:

1. Primary: radio frequency transmission to local receivers using existing UA antennas and modified C2 or video link protocols including one or more open standards

2. Secondary: Add-on modules that make use of one of the link protocols

3. Tertiary: Optional network-based identification system, likely over mobile telephone connections and the internet

## A Note on this Paper

DJI prides itself on working collaboratively on solutions with industry stakeholders and regulators. This whitepaper was prepared in response to AUVSI's call for papers, within a limited period of time, for discussion purposes. We look forward to receiving feedback and incorporating that feedback into a future revision of this paper.

## Appendix A

### Response to AUVSI Areas

In this Appendix we briefly respond to AUVSI's specific inquiries in its call for papers.

Technology Description

- Overview of technology concept

**Response: The technology in consideration would make use of existing command-and-control equipment on board the UA to send identification and position information to a radio receiver, using a protocol to add identification information to the downlink.**

Technology Operational Concept

- Describe how it would be employed and the user interface application

**Response: Law enforcement and others would view an electronic map of the surrounding area and be able to identify UA operating within radio range.**

- Describe supporting infrastructure (e.g. internet)

**Response: No infrastructure is required.**

- Define Technology Readiness Level (when could it be fielded for testing/initial operations)

**Response: There could be some level of readiness for initial operations this summer.**

- Describe reliability assurance and continuity of service features

**Response: This approach would be reliable when the UA is within range of the receiver. There is no server or network posing continuity issues.**

- Describe utilization of readily available spectrum/communication network(s) (e.g. LTE)

**Response: No additional spectrum is required beyond what the UA already uses for command-and-control.**

- Highlight limiting factors

**Response: Distribution of receivers and the creation of one or more common transmission protocols.**

Airborne Component: Describe component(s)/technology that would be on the vehicle. Must be technologies that will work on a SUAS vehicle (<55lbs).

- Light weight
- Low power (power source)
- Miniaturized in size
- Rough order of cost (must be affordable for vehicle equipage)

**Response: For UA with compatible control links, no additional weight or power because the solution uses existing radio equipment. For UA with other control links, perhaps an add-on RF module at low cost. We do not have a specific cost given that this is a whitepaper. 2.4 GHz is a common ISM band for almost all "drones". Other links are likely to be licensed spectrum for larger, specialized UAS. As with UAS registration, there should be a lower limit on any requirement to identify, but this needs to be discussed in light of safety goals because the FAA registration cutoff of 250 grams strikes as too low, based on our refined analysis of the calculations performed by the FAA UAS Registration Task Force.**

Ground Component: Describe the ground component(s)/technology needed for identification and tracking of vehicle.

**Response: A radio receiver with a screen for display, which over time may be similar in cost to existing high-quality RC controllers and portable screens.**

# Appendix B

## Selections from Public Comments to FAA-2011-0183

"AOPA has significant concerns with the implications on an individual's privacy, confidentiality, security and personal safety that could result from the proposed changes. Further, it appears the proposed FAA action is a solution in search of a problem that doesn't exist without due regard for the adverse impact it may have on private individual citizens because of the unnecessary release of personal information. AOPA has determined that the proposed changes are dangerous, invasive and unwarranted and the unintended negative implications are far reaching."

- Melissa Rudinger, AOPA

"I don't feel it is anyone else's business where we go. It is not only a privacy issue, but when it comes to business it is a competitive issue. The competition just does not need to know what we are doing.
It is the same as tracking where you drive your car.
George Orwell was right on."

- Hal Shevers, Sportsman Market Inc.

"The principle concern among corporations is the safety and security of their employees. The change to the MOA, as proposed, would allow anyone who may have the desire to follow a person a mechanism through which they can do so real-time by tracking the movement of an aircraft. The safety and security implications for those persons would become unbounded by this type of information being made available to both the curious observer and those harboring illicit intentions. GAMA finds this to be unacceptable."

- Jens Hening, GAMA

"As a Chief Security Officer (CSO) for a Fortune 500 company, my primary concern with this regulation is the public facing information regarding where our senior employees travel from a security and risk perception (i.e., kidnap and ransom, sabotage, and competitive industrial espionage). Our corporation prides itself on ethics, corporate responsibility, and shareholder transparency and the current FAA rules demonstrate compliance in submitting flight plans. Where is the 'National Security' nexus between public record and compliance in confidence?"

- Pete Short

"The Notice is flawed for many reasons and should be withdrawn. First, the predicate for the BARR program since its inception has been as much to protect the privacy interests of private persons and businesses as it has been about the security of travelers. Yet the Notice belittles the privacy interests of air travelers."

- Greg Walden, Patton Boggs LLP (on behalf of an anonymous consumer packaged products manufacturer)

"Not only is this an unnecessary and irresponsible proposal, it sets a dangerous precedent for the privacy and safety of our customers. Here are a few examples of how this proposal would negatively impact people and businesses:

It tramples citizens' right to privacy
It facilitates electronic stalking by unknown third parties
It creates an unnecessary competitive vulnerability for American businesses
It singles out general aviation for punitive treatment. It remains illegal for Amtrak or the commercial airlines to make public the names of their passengers.
It sets a precedent for the government to disclose any private data about individuals that it collects."

- Dan Hinson, Hawker Beechcraft Corporation

"As a matter of security for our employees we do not want public access to our aircraft status and routes. We have no objection to governmental or law enforcement access to this information, but see no practical value for the public access and in fact consider this a major security issue as it could alert 'bad actors' as to the location and plans for our aircraft."

- David Barta, Cooper US

"Privacy of movement is a fundamental American value. I believe the federal government should, to the greatest extent possible, protect such information rather than transmit it to anyone in the world with a computer connection. With this proposal, the government is targeting for broadcast the movements of those individuals and companies who utilize general aviation airplanes, but the situation could just as easily involve individuals and companies who utilize an automobile with an E-Z Pass. I do not believe there is any mode of transportation where the public dissemination of private movements is warranted."

- Robert Moore, Hewlett-Packard

"An attractive woman is in the car next to you at the red light. You lag behind and take down her car registration and go to your state's DMV website, where they have the car owner's address available to anyone who puts in the registration number off the vehicle, right??
Wrong!"

- Dean Block

"It is completely un AMERICAN to have small planes tracked differently than cars. Why don't we track credit card use, bathroom use, and everything else. Komrade Stalin would be proud. Seriously, privacy is important. Please don't do this."

- Jay Locke

"Eliminating an aircraft operator's discretion to restrict real-time access to their aircraft whereabouts would be an inconsistent position with the government stance on similar data. If this change were to be enacted it could be argued that APIS or Secure Flight data should be similarly released so that all passenger manifests for private and airline flights to/from/within the United States should be released for public scrutiny."

- Daniel Baker, FlightAware

"…the Notice fails to identify any government interest whatsoever that would be advanced by preventing owners and operators of private aircraft from blocking the disclosure of flight tracking information to unknown persons."

- Edward Bolen, Jeffrey Shane, NBAA

"That the government would seek to undermine such a valuable safeguard without setting forth a compelling public policy rationale for doing so runs counter to the best interests of American business and the values and traditions of the Federal Government."

- Michael McCormick, Global Business Travel Association

"The FAA's newly proposed limitation ignores the legitimate need for the Block Aircraft Registration Request (BARR) Program, and runs directly counter to long-established assumptions about government's role in the protection of privacy."

- Melvin King, Honeywell Flight Operations